

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-257668

(43)Date of publication of application : 21.09.2001

(51)Int.Cl.

H04L 9/08  
G06F 15/00  
G06K 17/00  
G06K 19/073  
G09C 1/00  
H04L 9/32

(21)Application number : 2000-069794

(22)Date of filing : 14.03.2000

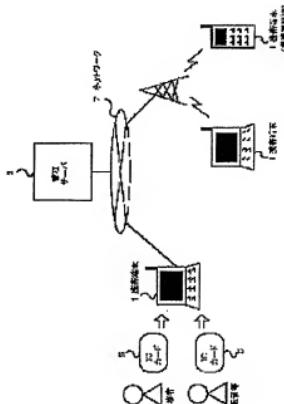
(71)Applicant : NTT DATA CORP

(72)Inventor : NIIMURA TAKAHIKO  
KOBAYASHI TAKAFUMI  
MACHIDA OSAMU

## (54) AUTHENTICATION SYSTEM, PORTABLE TERMINAL, CERTIFYING METHOD AND RECORDING MEDIUM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an authentication system having high flexibility.  
**SOLUTION:** An IC card 5 makes response to an access request from the other IC card 5 and obtains the authentication key (open key and the like) and access information of the IC card 5 being an access request source from a management server 3 managing the authentication keys and access information of all IC cards 5 through a terminal 1. The IC card 5 checks a signature from the access request source and an access instruction by using the obtained authentication key and access information. When a check result is normal, access from the other IC card 5 is permitted and the requested instruction is performed.



(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-257668

(P2001-257668A)

(43)公開日 平成13年9月21日(2001.9.21)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーブル <sup>7</sup> (参考)
H 04 L 9/08		G 06 F 15/00	3 3 0 G 5 B 0 3 5
G 06 F 15/00	3 3 0	G 06 K 17/00	E 5 B 0 5 8
G 06 K 17/00		G 09 C 1/00	6 4 0 B 5 B 0 8 5
19/073			6 6 0 A 5 J 1 0 4
G 09 C 1/00	6 4 0	H 04 L 9/00	6 0 1 D 9 A 0 0 1
			審査請求 未請求 請求項の数 9 O L (全 15 頁) 最終頁に続く

(21)出願番号 特願2000-69794(P2000-69794)

(71)出願人 000102728

株式会社エヌ・ティ・ティ・データ  
東京都江東区豊洲三丁目3番3号

(22)出願日 平成12年3月14日(2000.3.14)

(72)発明者 新村 貴彦  
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内(72)発明者 小林 孝文  
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内(74)代理人 100095407  
弁理士 木村 满

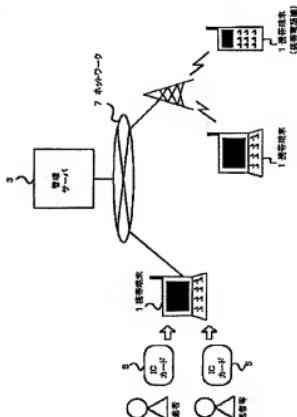
最終頁に続く

(54)【発明の名称】認証システム、携帯端末、認証方法及び記録媒体

(57)【要約】

【課題】柔軟性の高い認証システム等を提供することを目的とする。

【解決手段】ICカード5は、他のICカード5からのアクセス要求に応答し、アクセス要求元のICカード5の認証用鍵(公開鍵等)とアクセス情報を端末1を介して、全ICカード5の認証用鍵とアクセス情報を管理する管理サーバ3から取得する。ICカード5は、取得した認証用鍵とアクセス情報を用いて、アクセス要求元からの署名とアクセス命令をチェックする。チェック結果が正當である場合、他のICカード5からのアクセスを許可し、要求された命令を実行する。



## 【特許請求の範囲】

【請求項1】各ICカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第1のICカードへアクセスを要求する第2のICカードを認証するための認証システムであって、携帯端末のカード処理部にセットされた第1のICカードに対する第2のICカードからのアクセス要求に応答して、前記第2のICカードの認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、  
取得した認証用鍵とアクセス情報との少なくとも一方を用いて前記第2のICカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第1のICカードへのアクセスを許可する、  
ことを特徴とする認証システム。

【請求項2】各携帯端末の認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第1の携帯端末へアクセスを要求する第2の携帯端末を認証するための認証システムであって、  
第1の携帯端末に対する第2の携帯端末からのアクセス要求に応答して、前記第2の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、  
取得した認証用鍵とアクセス情報を用いて前記第2の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第1の携帯端末へのアクセスを許可する、  
ことを特徴とする認証システム。

【請求項3】前記携帯端末は、携帯電話機を含む、  
ことを特徴とする請求項1又は2に記載の認証システム。

【請求項4】各ICカードの認証に必要な認証情報を管理するセンタを備え、ICカード間の認証を行うための認証システムであって、  
各前記ICカードは、

コンテンツ情報を記憶し、  
他の前記ICカードからのアクセス要求に応答して、当該他のICカードの認証とアクセスレベルのチェックの少なくとも一方を含む認証処理を行い、  
前記認証処理の結果が正常を示す場合、コンテンツ情報をへのアクセスを許可し、

前記センタは、  
前記ICカードに、認証処理に必要な情報を供給する、  
ことを特徴とする認証システム。

【請求項5】アクセス要求元の認証を行う携帯端末であって、  
他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、各携帯端末の認証用鍵とアクセス情報との

少なくとも一方を記憶するサーバから通信により取得し、  
取得した認証用鍵とアクセス情報との少なくとも一方を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセスを許可する、  
ことを特徴とする携帯端末。

【請求項6】前記携帯端末は、携帯電話機を含む、  
ことを特徴とする請求項5に記載の携帯端末。

10 【請求項7】各ICカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備えるシステムにおける、第1のICカードへアクセスを要求する第2のICカードを認証するための認証方法であって、  
携帯端末のカード処理部にセットされた第1のICカードに対する第2のICカードからのアクセス要求に応答して、前記第2のICカードの認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、

20 取得した認証用鍵とアクセス情報を用いて前記第2のICカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第1のICカードへのアクセスを許可する、  
ことを特徴とする認証方法。

【請求項8】各携帯端末の認証用鍵とアクセス権限を示すアクセス情報を用いて前記第2の携帯端末からの署名とアクセス命令との少なくとも一方を記憶するサーバを備えるシステムにおける、第1の携帯端末へアクセスを要求する第2の携帯端末を認証するための認証方法であって、  
30 第1の携帯端末に対する第2の携帯端末からのアクセス要求に応答して、前記第2の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、  
取得した認証用鍵とアクセス情報を用いて前記第2の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第1の携帯端末へのアクセスを許可する、  
ことを特徴とする認証方法。

【請求項9】コンピュータを、アクセス要求元の認証を行う携帯端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、  
該コンピュータを、他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報を用いて、他の携帯端末からの署名とアクセス命令との

40 少なくとも一方を、各携帯端末の認証用鍵とアクセス情報を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方を記憶するサーバから通信により取得する手段、  
取得した認証用鍵とアクセス情報を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセス

を許可する手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ICカード等へのアクセス管理を行うための認証システム等に関するもの。

【0002】

【従来の技術】 近年、情報技術の進歩により、各利用者が自己のICカードを用いてサービスを受けることができるシステムが考案されている。これらのシステムでは、ICカードへの不正なアクセスを防止するために、アクセス要求元の正当性やアクセス権限等をチェックしていた。例えば、アクセス要求元のチェックでは、アクセス要求元から、そのアクセス要求元の秘密鍵等でなされた署名等をICカードが受け取り、相手の公開鍵を用いて署名の正当性をチェックしていた。

【0003】 また、アクセス権限のチェックでは、各ICカードにそれぞれ付与されているアクセス権限の情報を参照して、アクセス要求元からのアクセス命令が、適正なアクセス命令であるかをチェックしていた。例えば、あるICカードに、「Aデータ」へのアクセス権限として、データの読出のみが許可されている他のICカードから、データの書き込を要求するアクセス要求を受信した場合には、アクセス権限外のアクセス命令であるとして、アクセスを拒否していた。

【0004】

【発明が解決しようとする課題】 上記のような認証システムでは、各ICカード等は、アクセス要求元の認証を行なうために、システムの利用者の全てのICカードの認証用鍵とアクセス権限を示すアクセス情報とを保持しなければならない。しかし、各ICカードにおいて、これらの情報を全て記憶せることは実質上困難であった。このため、メモリに記憶される認証用鍵とアクセス情報のデータが削除されるため、結果的に、サービス内容や利用者数など、システムの利用に関して種々の制限が課されていた。また、ICカードに記憶される認証用鍵やアクセス情報が不正利用されないように、各カードの安全性等の機能を強化する必要があった。

【0005】 本発明は、上述した事情に鑑みてなされたもので、ICカードの記憶容量に基づくシステムの利用制限を軽減することができる認証システム等を提供することを目的とする。また、本発明は、ICカードの機能負担を軽減しつつ、システムの安全性を保持することができる認証システム等を提供することを目的とする。

【0006】

【課題を解決するための手段】 上記目的を達成するため、本発明の第1の観点に係る認証システムは、各ICカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第1のIC

カードへアクセスを要求する第2のICカードを認証するための認証システムであって、携帯端末のカード処理部にセットされた第1のICカードに対する第2のICカードからのアクセス要求に応答して、前記第2のICカードの認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、取得した認証用鍵とアクセス情報との少なくとも一方を用いて前記第2のICカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第1のICカードへのアクセスを許可することを特徴とする。

【0007】 このような構成によれば、例えば全ICカードの認証用鍵等をサーバで集中管理して、あるICカードにアクセス要求があった場合には、相手の認証に必要な情報はサーバから取得して認証処理を行う。これにより、ICカードに大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるICカード側の負担を軽減することができる。

【0008】 また、本発明の第2の観点に係る認証システムは、各携帯端末の認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第2の携帯端末へアクセスを要求する第2の携帯端末を認証するための認証システムであって、第1の携帯端末に対する第2の携帯端末からのアクセス要求に応答して、前記第2の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、取得した認証用鍵とアクセス情報を用いて前記第2の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第1の携帯端末へのアクセスを許可することを特徴とする。

【0009】 このような構成によれば、例えば全携帯端末の認証用鍵等をサーバで集中管理して、ある携帯端末にアクセス要求があった場合には、相手の認証に必要な情報はサーバから取得して認証処理を行う。これにより、多数の認証用鍵やアクセス情報を記憶するための大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるICカード側の負担を軽減することができる。

【0010】 また、第1と第2の観点に係る認証システムにおいて、前記携帯端末は、携帯電話機を含んでもよい。

【0011】 また、本発明の第3の観点に係る認証システムは、各ICカードの認証に必要な認証情報を管理するセンタを備え、ICカード間の認証を行うための認証システムであって、各前記ICカードは、コンテンツ情

報を記憶し、他の前記1Cカードからのアクセス要求に応答して、当該他の1Cカードの認証とアクセスレベルのチェックの少なくとも一方を含む認証処理を行い、前記認証処理の結果が正常を示す場合、コンテンツ情報へのアクセスを許可し、前記センタは、前記1Cカードに、認証処理に必要な情報を供給することを特徴とする。

【0012】また、本発明の第4の観点に係る携帯端末は、アクセス要求元の認証を行う携帯端末であって、他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、各携帯端末の認証用鍵とアクセス情報との少なくとも一方を記憶するサーバから通信により取得し、取得した認証用鍵とアクセス情報との少なくとも一方を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセスを許可することを特徴とする。

【0013】前記携帯端末は、携帯電話機を含んでもよい。

【0014】また、本発明の第5の観点に係る認証方法は、各1Cカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備えるシステムにおける、第1の1Cカードへアクセスを要求する第2の1Cカードを認証するための認証方法であって、携帯端末のカード処理部にセットされた第1の1Cカードに対する第2の1Cカードからのアクセス要求に応答して、前記第2の1Cカードの認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、取得した認証用鍵とアクセス情報との少なくとも一方を用いて前記第2の1Cカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第1の1Cカードへのアクセスを許可することを特徴とする。

【0015】このような構成によれば、例えば全1Cカードの認証用鍵等をサーバで集中管理して、ある1Cカードにアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、1Cカードに大容量のメモリを必要とせずに資源を効率よく使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおける1Cカード側の負担を軽減することができる。

【0016】また、本発明の第6の観点に係る認証方法は、各携帯端末の認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備えるシステムにおける、第1の携帯端末へアクセスを要求する第2の携帯端末を認証するための認証方法であって、第1の携帯端末に対する第2の携帯端末からのアクセス要求に応答して、前記第2の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介し

て前記サーバから取得し、取得した認証用鍵とアクセス情報を用いて前記第2の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第1の携帯端末へのアクセスを許可することを特徴とする。

【0017】このような構成によれば、例えば全携帯端末の認証用鍵等をサーバで集中管理して、ある携帯端末にアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、多段の認証用鍵やアクセス情報を記憶するための大容量のメモリを必要とせずに資源を効率よく使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおける1Cカード側の負担を軽減することができる。

【0018】また、本発明の第7の観点に係る記録媒体は、コンピュータを、アクセス要求元の認証を行う携帯端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを、他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、各携帯端末の認証用鍵とアクセス情報との少なくとも一方を記憶するサーバから通信により取得する手段、取得した認証用鍵とアクセス情報との少なくとも一方を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセスを許可する手段、として機能させるためのプログラムを記録する。

【0019】

【発明の実施の形態】以下、本発明に係る実施の形態を、病院等で使用される1Cカード認証システムを例に図面を参照して説明する。

【0020】本実施形態に係る1Cカード認証システムのシステム構成図を図1に示す。図示されるように、本システムは、携帯端末1と管理サーバ3と1Cカード5と、を備え、携帯端末1と管理サーバ3は、例えば公衆回線等のネットワーク7に接続される。

【0021】携帯端末1は、1Cカード5間のデータの授受、1Cカード5と管理サーバ3とのデータの授受等を行うための装置であり、例えば図2に示すように、制御部11と、カードリーダライタ部13と、記憶部15と、通信制御部17と、を備える。

【0022】制御部11は、カードリーダライタ部13に装着されている1Cカード5と、他の1Cカード5との間の情報の授受を制御等する。具体的には、制御部11は、カードリーダライタ部13に装着されている1Cカード5へのアクセス要求等を他のカードから受信した場合には、そのアクセス要求等を1Cカード5に送信する。例えば、カード挿入口を2つ備えるカードリーダラ

イタ部13にそれぞれICカード5が挿入され、一方のICカード5からのアクセス要求を受信して、他方のICカード5に送信してもよい。また、他の携帯端末1のカードリーダライタ部13にセットされたICカード5からのアクセス要求をネットワーク7等を介して受信して、自己のカードリーダライタ部13にセットされているICカード5に渡してもよい。

【0023】また、制御部11は、カードリーダライタ部13に装着されているICカード5から受信した種々の要求(認証情報要求、権限変更要求等)をネットワーク7を介して管理サーバ3に送信し、これらに対して管理サーバ3から送信されてくる情報を受信して、ICカード5に送信する。

【0024】カードリーダライタ部13は、ICカード5のデータの読み取り書き込みを行う。記憶部13は、他の携帯端末1又は管理サーバ3から受信した情報を記憶する。通信制御部15は、他の携帯端末1又は管理サーバ3とのデータ通信を制御する。

【0025】なお、携帯端末1は、上記機能を備える携帯電話機、PDA(Personal Digital Assistants)等を含む。

【0026】管理サーバ3は、本システムの利用者の公開鍵やアクセス権限を示すアクセス権限表を管理するコンピュータであり、図3に示すように、記憶部31と、制御部33と、通信制御部35と、を備える。

【0027】記憶部31は、本システムの全利用者のICカード5の公開鍵と、管理サーバ3の秘密鍵及び公開鍵と、アクセス権限表とを記憶する。本システムでは、各利用者は、例えば「医者」、「薬剤師」等の所定のグループに分類されており、所属するグループを特定するためのグループ1Dが付与されている。なお、本実施例では、「医者」のグループ1Dを「G1D10」、「薬剤師」のグループ1Dを「G1D20」とする。

【0028】アクセス権限表は、例えば図4に示すように、後述するICカード5に記憶される個人情報の各データ(名前情報、住所情報、カルテ情報、処方箋情報等)について、それぞれのアクセス権限がグループ1D毎に設定されている。例えば図4に示すアクセス権限表には、名前情報及び住所情報については、医者と薬剤師による読み出し可能であることが設定されており、カルテ情報及び処方箋情報については、医者による読み出し及び書き込みが可能であることが設定されている。なお、このアクセス権限表は、例えばシステム管理者により入力設定される。

【0029】制御部33は、携帯端末1から、検証情報要求としてユーザ1Dとグループ1Dを受信すると、受信したユーザ1Dに対応する公開鍵を記憶部31から読み出し、また、受信したグループ1Dに対応するアクセス情報を記憶部31におけるアクセス権限表から読み出す。そして、読み出した公開鍵及びアクセス情報を、管

理サーバ3の秘密鍵を用いた署名を付与して要求元の携帯端末1に送信する。

【0030】また、制御部33は、携帯端末1から権限変更要求を受信すると、記憶部31に記憶されているアクセス権限表から読み出した情報に、指定された変更を施したアクセス情報を要求元に送信する。この際、記憶部31に記憶されているアクセス権限表の内容には何ら変更を及ぼさない。権限変更要求には、所定グループのアクセス権限の追加を要求する権限追加要求と、所定グループのアクセス権限の削除を要求する権限削除要求と、新たなグループについてアクセス情報の登録を要求する登録要求等がある。

【0031】権限追加要求は、変更対象グループのグループ1Dと、追加対象のコマンド(例えば、「カルテ情報を読み出す」と)、を含む。制御部33は、この権限追加要求を受信した場合、受信したグループ1Dのアクセス情報を記憶部31のアクセス権限表から所定の記憶領域にコピーし、コピーされたアクセス情報に、受信したコマンドを追加する処理を行う(該当するデータ種別が「読み出」であることを設定する)。そして、コマンドが追加されたアクセス情報に管理サーバ3の秘密鍵を用いた署名を付して、要求元の携帯端末1に送信する。

【0032】また、権限削除要求は、変更対象グループのグループ1Dと、削除対象のコマンドと、を含む。制御部33は、この権限削除要求を受信した場合、受信したグループ1Dのアクセス情報を記憶部31のアクセス権限表から所定の記憶領域にコピーし、コピーされたアクセス情報を、受信したコマンドを削除する処理を行う。そして、コマンドが削除されたアクセス情報に管理サーバ3の秘密鍵を用いた署名を付して、要求元の携帯端末1に送信する。

【0033】また、登録要求は、登録対象のグループ1Dと、登録対象のコマンドと、を含む。制御部33は、この登録要求を受信した場合、受信したグループ1Dについてアクセス情報を作成し、これに管理サーバ3の秘密鍵を用いた署名を付して、要求元の携帯端末1に送信する。

【0034】なお、ICカード5が管理サーバ3に所定の権限変更のための書換命令発効依頼を送信し、管理サーバ3がこれに応じた書換命令をICカード5に送信し、これに応じて、ICカード5が自己の保持するアクセス情報を書き換えるようにしてよい。

【0035】また、制御部33は、携帯端末1からアクセス権限表の参照要求を受信すると、記憶部31に記憶されているアクセス権限表に格納されているアクセス情報を読み出して、管理サーバ3の署名を付与して要求元の携帯端末1に送信する。また、参照要求とともに参照対象のグループ1Dを受信した場合には、制御部33は、指定されたグループ1Dに対応するアクセス情報を読み出して要求元の携帯端末1に送信する。また、通信

制御部35は、各携帯端末1とのデータ通信を制御する。

【0036】ICカード5は、本システムの利用者がそれぞれ保持するカードであり、MPU、ROM、RAM、EEPROM等を有するICチップを備える。ICチップは、例えば図5に示すように、MPUがROM等に記憶されるプログラムを実行することにより実現される制御部51とメモリ52と入出力制御部53とを備える。

【0037】制御部51は、そのICカード5へのアクセスが要求された場合に、アクセス要求元である相手の認証及びアクセス権限の検証等を行う。この認証処理では、制御部51は、まず携帯端末1を介して他のICカード5からのアクセス要求を受信する。アクセス要求は、例えばアクセス要求元である相手のユーザIDとグループIDとアクセスコマンド等を含む要求情報と、署名等を含む。なお、この実施例でのアクセスコマンドとは、アクセス要求元が要求するアクセスの種別を示し、例えば「カルテ情報を読み出す」、「処方箋情報を書き込む」等のコマンドを示す。

【0038】次に、制御部51は、受信したアクセス要求における要求情報に含まれるユーザIDとグループIDについて、これらを含む検証情報要求を生成し、携帯端末1を介して管理サーバ3から送信する。そして、これに応答して管理サーバ3から送信されてくる検証情報(アクセス要求元の公開鍵とアクセス情報を含む)を携帯端末1から受け取ってメモリ52に記憶する。

【0039】制御部51は、管理サーバ3から取得したアクセス要求元の公開鍵を用いて、アクセス要求における署名を復号化し、復号化結果が要求情報と合致するかを判定する等して、アクセス要求元の正当性をチェックする。

【0040】また、制御部51は、アクセス要求元のグループIDに基づいて、該当するグループIDのアクセス情報を参照し、アクセスが要求されているデータについて、要求されたコマンドの実行が許可されているか否かを判断する。例えばグループID「G1D10」の要求元から受信した「カルテ情報を読み出す」というアクセスコマンドを検証する場合には、制御部51は、「グループID「10」のアクセス情報を参照し、「カルテ情報を読み出す」の権限が「読み出可」であることをチェックする。

【0041】そして、署名の認証とアクセスコマンドの検証が正常に完了すると、制御部51は、アクセス要求元からのアクセスコマンドを実行する。アクセスコマンドが例えば「カルテ情報を読み出す」等の所定情報の読み出命令である場合、制御部51はメモリ52から指定された情報を読み出し、携帯端末1を介してアクセス要求元のICカード5に送信する。また、アクセスコマンドが例えば「処方箋情報を書き込む」等の所定情報の書き込み

令である場合、制御部51は、その命令とともに受信した所定情報をメモリ52に記憶する。

【0042】また署名の認証結果がエラーとなった場合、又は、アクセスコマンドの検証がエラーとなった場合には、制御部51は、所定のエラー信号をアクセス要求元のICカード5に携帯端末1を介して送信する。

【0043】また、制御部51は、そのICカード5の保持者(利用者)からの要求に応じて、所定グループのアクセス権限の変更を管理サーバ3に要求するアクセス権限変更処理を行う。このアクセス権限変更処理では、制御部51は、例えばPINの入力チェックにより本人確認を行ったのち、利用者から入力された、変更内容(権限の追加、権限の削除、新規登録等)と、変更対象のコマンド(追加、削除、登録等)と、変更対象グループのグループID等を携帯端末1から受け取る。そして、その入力データに応じて、グループIDとコマンドを含む権限変更要求(権限追加要求、権限削除要求、登録要求等)を作成し、携帯端末1を介して管理サーバ3に送信する。そして、この権限変更要求に応答して管理

20 サーバ3から送信されてきた変更後のアクセス情報をメモリ52に記憶する。なお、このアクセス情報の変更は、管理サーバ3の記憶部31に記憶されているアクセス情報には反映されない。

【0044】また、制御部51は、そのICカード5の保持者からの要求に応じて、管理サーバ3で管理されているアクセス権限表の参照要求を送信する。制御部51は、アクセス権限表に格納されている全アクセス情報を要求してもよく、また、カード保持者からの1又是複数のグループIDの入力を受けて、入力されたグループIDに対応するアクセス情報の参照を管理サーバ3に要求してもよい。制御部51は、この参照要求に応答して管理サーバ3から受信したアクセス情報を例えば携帯端末1を介して表示する。

【0045】また、制御部51は、他のICカード5へアクセス要求を送信するアクセス要求処理を行う。制御部51は、アクセスコマンドと、自己のユーザID及びグループIDを含む要求情報を自己の秘密鍵を用いた署名を付与したアクセス要求を生成し、アクセス要求元のICカード5に割り当てられる。

【0046】メモリ52は、例えば、図6(A)に示すよう、そのICカード5に付与された秘密鍵及び公開鍵、ユーザID、グループID、管理サーバ3の公開鍵等の初期情報と、例えば図6(B)に示すよう、カード保持者の個人情報(例えば、名前情報、住所情報、カルテ情報、処方箋情報等)等を記憶する。また、メモリ52は、例えば図7(A)に示すよう、管理サーバ3から取得した認証相手先の公開鍵をユーザIDとともに記憶し、また、図6(B)に示すよう、管理サーバ3から取得したアクセス情報をグループID毎に記憶する。

【0047】各ICカード5の秘密鍵及び公開鍵は、例えば各ICカード5が、カード内で自己用の秘密鍵及び公開鍵を生成し、そのうちの公開鍵を携帯端末1を介して管理サーバ3に登録する。また、管理サーバ3が、各ICカード5について秘密鍵及び公開鍵を生成し、そのうちの秘密鍵を格納した記録媒体を各利用者に配布してもよい。また、秘密鍵を暗号化して、通信により携帯端末1を介して各ICカード5に送信してもよい。

【0048】出入力制御部53は、携帯端末1とのデータ通信を制御する。

【0049】次に、本システムの動作について、ICカード5間の通信及びICカード5と管理サーバ3との通信を中心に、例えば患者Aが病院に行って医者Bの診察を受け、診察後、薬剤師Cから薬をもらう場合を例に説明する。

【0050】本システムでは、患者Bが患者AのICカード5Aにアクセスして、カード内に記憶されているカルテ情報を読み取るためには、医者BのICカード5Bが患者AのICカード5Aによる認証を受ける必要がある。このカルテ情報を読み取るための認証処理について図8を参照して説明する。

【0051】まず、患者Aは、自己のICカード5Aを、例えば携帯端末1の第1のカード挿入口にセットする。また、医者Bは、自己のICカード5Bを、携帯端末1の第2のカード挿入口にセットし、例えば相手(患者A)のICカード5Aに記憶されているカルテ情報を見ることの要求を入力する。このときの入力方法は任意であり、医者が「カルテ情報を見る」というコマンドを直接入力してもよい、また、医者のアクセス権限を示すアクセス情報を携帯端末1が管理サーバ3から取得して表示し、その中から選択させてよい。携帯端末1は、入力(又は選択)された「カルテ情報を読み出す」というアクセスコマンドを医者BのICカード5Bに送信する。

【0052】これに応答して、ICカード5Bは、アクセスコマンド「カルテ情報を読み出す」と、例えばメモリ52から読み出した医者BのユーザID「U1D1」及びグループID「C1D10」を含む要求情報を生成し、また、この要求情報を自己の秘密鍵KEYS1を用いて署名を生成する。署名の生成方法は任意であり、例えば要求情報のハッシュ値を秘密鍵で暗号化して生成してもよい。そして、ICカード5Bは、生成した要求情報に署名を付与したアクセス要求S1を、患者AのICカード5Aに携帯端末1を介して送信する(L1)。

【0053】患者AのICカード5Aは、ICカード5Bからのアクセス要求S1を受信する。ICカードAは、例えばアクセス要求S1における要求情報を含まれるユーザID「U1D1」に対する公開鍵と、グループID「C1D10」に対するアクセス情報が未取得であることをメモリ52を参照して確認した後、ユーザID

12  
D「U1D1」とグループID「C1D10」を含む検証情報要求を、携帯端末1を介して管理サーバ3に送信する(L2)。

【0054】管理サーバ3は、受信したユーザID「U1D1」に対応する公開鍵「KEYP1」と、受信したグループID「C1D10」に対応するアクセス情報と、を記憶部31からそれぞれ読み出し、これらの情報に、管理サーバ3の秘密鍵KEYSCAを用いて生成した署名を付した検証情報SCAを携帯端末1を介して13  
Cカード5Aに送信する(L3)。

【0055】ICカード5Aは、管理サーバ3から受信した検証情報SCAにおける署名を管理サーバ3の公開鍵KEYP1を用いて確認した後、受信した公開鍵「KEYP1」を用いてICカード5Bからのアクセス要求S1における署名をチェックする。署名のチェック方法は任意であり、例えば管理サーバ3から取得した公開鍵で署名を復号化した結果が、要求情報のハッシュ値と合致するかを判別してもよい。

【0056】ICカード5Aは、ICカード5Bによる署名の正当性を確認すると、次に、管理サーバ3から取得したユーザID「U1D10」のアクセス情報を参照し、アクセス対象の「カルテ情報」について設定されているアクセス権限が、アクセスコマンドと合致するかを判断する。なお、この例において管理サーバ3が記憶するアクセス権限表は、例えば図2に示すアクセス権限表と同様の内容を有することとする。従って、グループ1D「C1D10」のアクセス情報の「カルテ情報」のアクセス権限表「読出」と「書込」の双方が許可されているため、カルテ情報を読み出しを要求するアクセスコマンドを合致すると判断される。

【0057】ICカード5Bからのアクセス要求S1における署名とアクセスコマンドのチェックが正常に完了すると、ICカード5Aは、アクセスコマンド「カルテ情報を読み出す」を実行し、実行結果をICカード5Bに返す(L4)。この場合、ICカード5Aがメモリ52から患者Aのカルテ情報を読み出し、携帯端末1を介してICカード5Bに送信する。そして、ICカード5Bが、受信したカルテ情報を所定の表示要求とともに携帯端末1に送信して表示させる。また、ICカード5AからICカード5Bへは実行結果が正常である旨のOK信号を送信し、カルテ情報は、ICカード5Aから携帯端末1へ所定の表示要求とともに送信されるようにしてよい。これにより、医者Bが患者AのICカード5Aに記憶されるカルテ情報を読み取ることができる。

【0058】なお、署名の認証とアクセスコマンドの検証の少なくとも一方がエラーとなった場合、ICカード5Aは、所定のエラー信号をICカード5Bに送信する。また、アクセスコマンドを実行した際にエラーが発生した場合には、ICカード5Aは、実行結果として所定のエラー信号をICカード5Bに送信する。

【0059】患者Aのカルテ情報を読み、患者Aの診察を行った医者Bは、患者AのICカード5Aにアクセスして、患者Aの診察結果をカルテ情報として記録しようとする。このカルテ情報を記録するための認証処理について図9を参照して説明する。

【0060】例えば患者AのICカード5Aと医者BのICカード5Bは、上記と同様に、携帯端末1の各カード插入口にセットされていることとする。医者Bは、診察結果情報と、患者AのICカード5Aにカルテ情報を記録することの要求を入力する。携帯端末1は、この入力に応答して、診察結果情報と「カルテ情報を書き込む」というアクセスコマンドを、医者BのICカード5Bに送信する。

【0061】ICカード5Bは、受信した診察結果情報、アクセスコマンド「カルテ情報を書き込む」、医者BのユーザID「UID1」及びグループID「GID10」を含む要求情報に、自己の秘密鍵KEYS1を用いた署名を付与してアクセス要求S1を生成し、患者AのICカード5Aに携帯端末1を介して送信する(L1)。

【0062】患者AのICカード5Aは、ICカード5Bからのアクセス要求S1を受信する。ICカード5Aは、先の認証処理(図8)で、ユーザID「UID1」に対応する公開鍵と、グループID「GID10」に対応するアクセス情報を既に管理サーバ3から取得しているため、管理サーバ3に対するこれらの情報の要求は行わない。ICカード5Aは、ユーザID「UID1」に対応する公開鍵「KEYP1」を用いて署名をチェックし、また、グループID「GID10」に対応するアクセス情報を用いてアクセスコマンドをチェックする。

【0063】そして、ICカード5Bからのアクセス要求S1における署名とアクセスコマンドのチェックが正常に完了すると、ICカード5Aは、ICカード5Bから受信したデータ(診察結果情報)をカルテ情報としてメモリ52記録することにより、アクセスコマンド「カルテを書き込む」を実行する。そして、実行結果(OK信号又はエラー信号)をICカード5Bに返す(L1-2)。これにより、医者Bは、認証を受けた後、患者Aの診察結果を、患者AのICカード5Aに記録することができる。

【0064】また、処方箋情報の記録も、上記のカルテ情報の記録と同様に処理される。この場合、ICカード5Bからのアクセス要求は、医者BのユーザID、グループID、アクセスコマンド「処方箋情報を書き込む」、医者Bにより入力された処方箋情報を含む。これにより、医者Bは、患者Aに対する処方箋情報を患者AのICカード5Aに記憶させることができる。

【0065】次に、患者Aは、薬をもらうために薬局に行く。薬剤師Cが患者AのICカード5Aにアクセスして、カード内に記憶されている処方箋情報を読みたま

に、薬剤師CのICカード5Cが患者AのICカード5Aによる認証を受ける必要がある。この処方箋情報を読むための認証処理について説明する。

【0066】まず、患者Aは、自己のICカード5Aを、携帯端末1の第1の挿入口にセットする。また、薬剤師Cは、自己のICカード5Cを、携帯端末1の第2の挿入口にセットし、例えば相手(患者A)のICカード5Aに記憶されている処方箋情報を見ることの要求を入力する。携帯端末1は、この入力に応答して、「処方箋情報を読み出す」というアクセスコマンドを薬剤師CのICカード5Cに送信する。

【0067】これに応じて、ICカード5Cは、受信したアクセスコマンド「カルテ情報を読み出す」と、例えばメモリ52から読み出した薬剤師CのユーザID「UID2」及びグループID「GID20」を含む要求情報と、この要求情報と自己の秘密鍵KEYS2を用いた署名を生成する。そして、図10に示すように、ICカード5Cは、要求情報に署名を付与したアクセス要求S2を、患者AのICカード5Aに携帯端末1を介して送信する(L2)。

【0068】患者AのICカード5Aは、ICカード5Cからのアクセス要求S2の受信に応答し、例えばアクセス要求S2における要求情報に含まれるユーザID「UID2」に対する公開鍵と、グループID「GID20」に対するアクセス情報をが未取得であることをメモリ52を参照して確認した後、ユーザID「UID2」とグループID「GID20」を含む検証情報要求を、携帯端末1を介して管理サーバ3に送信する(L2-2)。

【0069】管理サーバ3は、受信したユーザID「2」に対応する公開鍵「KEYP2」と、受信したグループID「GID20」に対応するアクセス情報を、を記憶し3から読み出し、これらの情報に、管理サーバ3の秘密鍵KEYSCAを用いて生成した署名を付した検証情報SCAを携帯端末1を介してICカード5Aに送信する(L2-3)。

【0070】ICカード5Aは、管理サーバ3から受信した検証情報SCAにおける署名を管理サーバ3の公開鍵KEYPCA用いて確認した後、ユーザID「UID2」に対応する公開鍵「KEYP2」を用いてアクセス要求S2における署名の正当性をチェックする。また、グループID「GID20」のアクセス情報を参照して、アクセス対象の「処方箋情報」について設定されているアクセス権限が、アクセスコマンドと合致するかをチェックする。なお、この例においても管理サーバ3が記憶するアクセス権限表は、例えば図2に示すアクセス権限表と同様の内容とする。従って、グループID「GID20」のアクセス情報の「処方箋情報」についてではアクセス権限が何ら許可されておらず、アクセスコマンドとは合致しない。この場合、ICカード5A

は、アクセス権限エラーを示すエラー信号をICカード5Cに送信する。

【0071】このようにアクセス要求がエラーとなった場合、患者Aは、薬剤師Cが処方箋情報を見ることができるように薬剤師Cの権限を変更することができる。この場合、患者Aは、例えばPINの入力チェックにより本人確認を行ったのち、所定グループのアクセス情報を追加変更する要求と、変更対象である薬剤師CのグループID「G1D20」と、追加したいコマンド「処方箋情報を読み出す」と、を入力し、携帯端末1は、入力された情報をICカード5Aに送信する。なお、薬剤師Cのグループの指定方法は任意であり、例えば上記のようにアクセス権限のチェックでエラーが発生した後に本処理を実行する場合には、エラーとなったグループのグループIDがICカード5A内で自動的に設定されてもよい。

【0072】ICカード5Aは、図11に示すように、薬剤師CのグループID「G1D20」、追加対象コマンド「処方箋情報を読み出す」等を含む権限追加要求を管理サーバ3に送信する（L31）。管理サーバ3は、権限追加要求を受信すると、受信したグループID「G1D20」のアクセス情報を記憶部31のアクセス権限表から読み出して、所定記憶領域等コピーする。そして、その読み出したアクセス情報を対して、コマンド「処方箋情報を読み出す」の追加処理を行う。そして、コマンドが追加された新たなアクセス情報を、管理サーバ3の秘密鍵KEYSCAを用いた署名を付してICカード5Aに送信する（L32）。なお、このとき、記憶部31に記憶されるアクセス権限表のアクセス情報は更新しない。

【0073】ICカード5Aは、アクセス権限が追加変更されたグループID「G1D20」を受信してメモリ52に記憶する。これにより、患者AのICカード5Aに記憶される薬剤師Cのアクセス権限が変更される。

【0074】なお、ICカード5Aが管理サーバ3にグループID「G1D20」のアクセス権限変更のための書換命令を発効依頼を送信し、管理サーバ3がこれに応じて、「G1D20」のアクセス情報をについての書換命令をICカード5に送信し、これに応じて、ICカード5Aがメモリ52に記憶されている「G1D20」のアクセス情報を書き換えるようにしてよい。

【0075】次に、アクセス権限が変更された薬剤師CはICカード5Aに記憶されている処方箋情報を見ることの要求を入力する。携帯端末1は、この入力された「処方箋情報を読み出す」というアクセスコマンドをICカード5Cに対して送信する。これに応答して、ICカード5Cは、図12に示すように、アクセスコマンド「処方箋情報を読み出す」、薬剤師CのユーザID「U1D2」及びグループID「G1D20」を含む要求情報に、自己の秘密鍵KEYS2を用いた署名を付与して

アクセス要求S2を生成し、患者AのICカード5Aに携帯端末1を介して送信する（L41）。

【0076】患者AのICカード5Aは、ICカード5Cからのアクセス要求S2を受信する。ICカード5Cは、先の認証処理及びアクセス権限変更処理（図10、図11）で、ユーザID「U1D2」に対応する公開鍵と、グループID「G1D20」の変更後のアクセス情報を既に取得しているため、管理サーバ3に対するこれらの情報の要求は行わない。ICカード5Aは、ユーザID「U1D2」に対応する公開鍵「KEYP2」を用いて署名をチェックし、また、グループID「G1D20」のアクセス情報を参照して、「処方箋情報」について設定されているアクセス権限が、アクセスコマンドと合致するかをチェックする。この場合、アクセス情報を「処方箋情報を読み出す」旨のアクセス権限が追加されたため、チェック結果は正常を示す。

【0077】そして、ICカード5Cからのアクセス要求S2における署名とアクセスコマンドのチェックが正常に完了すると、ICカード5Aは、アクセスコマンド「処方箋情報を読み出す」を実行し、実行結果をICカード5Cに返す（L42）。例えば、ICカード5Aがメモリ52から患者Aの処方箋情報を読み出し、携帯端末1を介してICカード5Cに送信する。そして、ICカード5Cが、受信した処方箋情報を所定の表示要求とともに携帯端末1に送信して表示させる。また、ICカード5AからICカード5Cへは実行結果が正常である旨のOK信号を送信し、処方箋情報は、ICカード5Aから携帯端末1へ所定の表示要求とともに送信されるようしてよい。これにより、薬剤師Cのアクセス権限の変更を行って、患者AのICカード5Aに記憶される処方箋情報を薬剤師Cが読みることができる。

【0078】なお、薬剤師Cについて追加したアクセス権限が今後不要ない場合には、ICカード5Aが、コマンド「処方箋情報を読み出す」の削除を要求する権限変更要求を管理サーバ3に送信してコマンドの削除を行ってよい。また、削除せずにこのままにしておけば、以後もオンラインで薬剤師CのICカード5Cの検証が可能となる。

【0079】このようにして、全ICカード5の認証用の鍵（公開鍵）やアクセス権限の情報を管理サーバ3で集中管理し、各ICカード5Aは、相手の認証に必要な情報（公開鍵、アクセス情報を）を管理サーバ3から取得して認証チェックを行なう。これにより、ICカードに大容量のメモリを必要とすることなく、ICカードの資源を効率良く使用できる。また、システムにおけるICカード側の負担を軽減した認証システムを実現することができる。また、システムの安全性及びメンテナンス性を向上することができる。

【0080】また、上記説明では、カード保持者が、自己のICカード5に記憶するアクセス情報をについて、各

グループに付与されているアクセス権限を変更することができるようになっているが、例えばカルテ情報等のように大事なデータは第三者（カルテ情報であれば医者等）の署名をつけて利用者（患者）のICカード5に記憶させるようにして、データの書換を防止してもよい。また、利用者からの要求により、各利用者のICカード5から管理サーバ3に依頼した命令（要求）等はログを取ることができるようにしてもらよい。そして、取ったログを不正使用の調査等に用いてもらよい。

【0081】また、ICカード5間の通信手段となる携帯端末1及びネットワーク7の使用形態は任意である。例えば、患者が病院で検査を受けて、その数日後に検査結果を受け取る場合に、検査結果を示すカルテ情報と処方箋情報を、自宅や職場等の任意の場所で、有線又は無線通信により携帯端末1で受信し、患者のICカード5に記録することもできる。この場合、例えば医者のICカード5から患者のICカード5へのアクセス要求が所定サーバに格納され、患者が携帯端末1から所定サーバにアクセスして自己宛のアクセス要求を取得する。所定サーバが、アクセス要求が登録されたことを検出して、所定の宛先に、登録されたアクセス要求を送信してもよく、又、アクセス要求が登録されたことの通知を送信してもよい。患者のICカード5は、上記説明と同様にして、取得したアクセス要求について署名及びアクセス権限の認証を行った後、ICカード5に検査結果を示すカルテ情報や処方箋情報を記録する。

【0082】そして、ICカード5に記録された処方箋情報をのみを販売から遠隔的にアクセスさせて、薬を患者に送付してもらうようにしてもらよい。患者の処方箋情報をアクセスする処理を自動化して、薬の販売が24時間可能な自動販売機や薬販売受付サービスを実現してもよい。また、患者が、自分で体重、血圧等の測定を行い、測定情報を病院に送信し、病院側で患者の認証を行った後、検査、分析等に用いてもらよい。無線通信機能を備える携帯端末（携帯電話機）を用いることにより、患者は外出先等でも検査結果を示すカルテ情報や処方箋情報を受け取ることができ、その利用場所が制限されることがないため、利便性はさらに向上する。

【0083】また、上記説明ではアクセス要求元の認証処理をICカード5内で行っていたが、この認証機能を管理サーバ3にも持たせても良い。この場合、他のICカード5からのアクセス要求を受信したICカード5は、受信したアクセス要求を管理サーバ3に送信する。管理サーバ3は、受信したアクセス要求に含まれるユーザIDとグループIDに応する公開鍵とアクセス情報を記憶部31から読み出し、ICカード5による認証処理と同様にして、アクセス要求に含まれる署名とアクセスコマンドをチェックし、チェック結果をICカード5に送信する。ICカード5は、管理サーバ3からのチェック結果が正常を示す場合には、アクセスコマンドを実

行し、チェック結果がエラーである場合には、エラー信号をアクセス要求元に返す。

【0084】また、上記説明では、アクセス対象となる情報（個人情報）を記憶するICカード5と、ICカードの通信手段となる携帯端末1とを用いるようにしているが、これに限定されず、ICカード5を用いて、上記のICカード5の機能をさらに有する携帯端末1を用いてもよい。この場合、携帯端末1は、例えば、上記説明においてICカード5に記録されていた秘密鍵及び公開鍵、個人情報を記憶部15に記憶し、アクセス要求の作成・送受信、アクセス要求元の認証、管理サーバ3との送受信、アクセスコマンドの実行等を行う。

【0085】ICカード5と管理サーバ3との間の通信は、安全上、暗号を用いることが望ましい。例えば、ICカード5が乱数を発生させ、この乱数を他の情報とともに管理サーバ3に送信し、管理サーバ3が署名対象の情報にICカード5から受信した乱数を含めて署名を行ない、ICカード5が管理サーバ3から受信した署名に含まれる乱数を確認するようにしてもらよい。これにより、割り込みによる偽メッセージの送受信を防ぐことができる。

【0086】また、本システムは、病院用の認証システムに限定されず、例えば電子マネーを記憶するICカードを用いる電子マネー・システム、個人情報を記憶するICカードを用いて住民票の発行等の行政サービスを行う行政システム等、認証処理を行う種々のシステムに適用され得る。

【0087】また、本発明を用いて、例えば、ICカードにコンテンツを格納し、インターネット上のホームページにアクセスするとの同様に、ICカードに格納されたコンテンツにアクセスするシステムを実現してもよい。例えば、利用者Aが利用者BのICカードに格納されているコンテンツを見たい場合には、利用者Aは携帯端末等に自己のICカードをセットして、利用者BのICカードに対してアクセス要求を送信する。利用者Bの端末は、利用者AのICカードからのアクセス要求を受信すると、上記説明と同様にして、署名及びアクセス権限をチェックし、チェック結果が正常を示せばアクセスを許可し、利用者Bは、利用者Bのコンテンツを例えばインターネットシステムにおけるコンテンツを管理するWWWサーバ等を必要とすることなく、携帯端末とICカード等の簡易な構成でネットワークを介した情報提供サービスを実現することができる。この場合、例えば複数の回線を使用する等して、複数の利用者からのアクセス要求を受け付け可能としてもよい。また、アクセス者からの要求に応じて、コンテンツ提供者がそのアクセス者と会話できるようにしてもらよい。この場合、例えば、アクセス要求元から所定の電話要求の受信に応じて、携帯電話機等のデータ送受信モードを電話モードに切り換え

て、所定のデータ送受信の手続に従って音声データを送受信する。

【0088】なお、ICカード5に記憶されるコンテンツ等を所定の鍵で暗号化しておき、管理センタ3からアクセスOKの指令が出たとき、又は、カード内で認証結果が確認されたとき、管理センタ3からのコンテンツ復号用の鍵を受け取って、アクセス対象のデータを復号化してもよい。

【0089】なお、この発明のICカード認証システムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体(フロッピー(登録商標)ディスク、CD-ROM等)から該プログラムをインストールすることにより、上述の処理を実行する携帯端末1、管理サーバ3等を構成することができる。なお、上述の機能を、OSが分担又はOSとアプリケーションの共同により実現する場合等には、OS以外の部分のみを媒体に格納してもよい。

【0090】なお、搬送波にプログラムを重複し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワークの掲示板(BBS)に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、OSの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【0091】  
【発明の効果】以上説明したように、本発明によれば、ICカード等の認証用鍵等をサーバで集中管理してあるICカード等にアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、多数の認証用鍵やアクセス情報を記憶するための大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるICカード側の負担等を軽減することができる。

【図面の簡単な説明】

\* 【図1】本発明の実施の形態に係るICカード認証システムのシステム構成図である。

【図2】図1のICカード認証システムで使用される携帯端末の構成を説明するための図である。

【図4】アクセス権限表を説明するための図である。

【図5】ICカードに記憶される初期情報と個人情報を説明するための図である。

【図6】ICカードに記憶される初期情報と個人情報を説明するための図である。

【図7】ICカードに記憶される公開鍵とアクセス情報を説明するための図である。

【図8】患者のICカードが医者のICカードを認証する場合の処理を説明するための図である。

【図9】患者のICカードが認証するための図である。

【図10】患者のICカードが薬剤師のICカードを認証する場合の処理を説明するための図である。

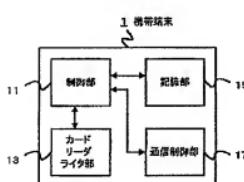
【図11】患者のICカードが薬剤師のアクセス権限を変更する場合の処理を説明するための図である。

【図12】患者のICカードが薬剤師のICカードを認証する場合の処理を説明するための図である。

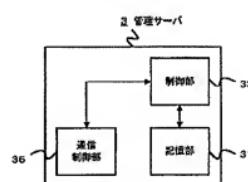
【符号の説明】

1	携帯端末
1 1	制御部
1 3	カードリーダライタ部
1 5	記憶部
1 7	通信制御部
3	管理サーバ
3 1	記憶部
3 3	制御部
3 5	通信制御部
5	ICカード
5 1	制御部
5 2	メモリ
5 3	入出力制御部
*	ネットワーク
7	

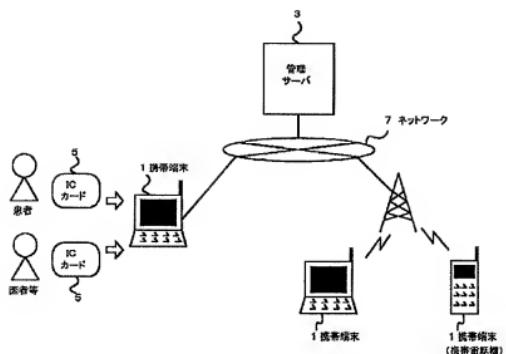
【図2】



【図3】



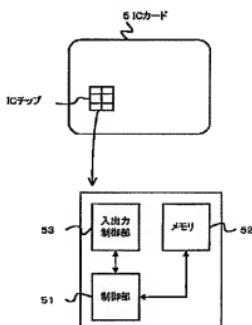
【図1】



【図4】

アクセス権限表		
グループID	アクセス情報	
GID10 (患者)	名前情報	読み出可
	住所情報	読み出可
	カルテ情報	読み出／書き込可
	双方面情報	読み出／書き込可
	...	...
	...	...
GID20 (医療機関)	名前情報	読み出可
	住所情報	読み出可
	カルテ情報	—
	双方面情報	—
	...	...
	...	...

【図5】



【図6】

(A) 初期情報		(B) 個人情報	
秘密鍵		名前情報	
公開鍵		住所情報	
ユーザID		カルテ情報	
グループID		施設情報	
管理サーバの公開鍵		...	...
...		...	...

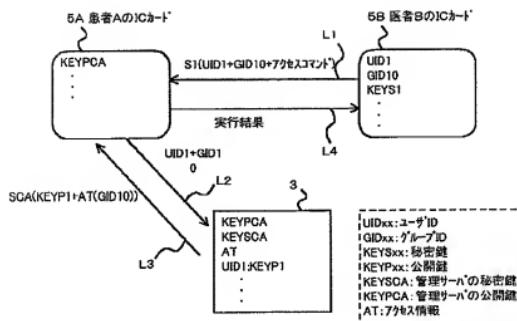
【図7】

(A) ユーザIDと公開鍵	
UserID	公開鍵
XXXXXXX	XXXXXXX
...	...
...	...

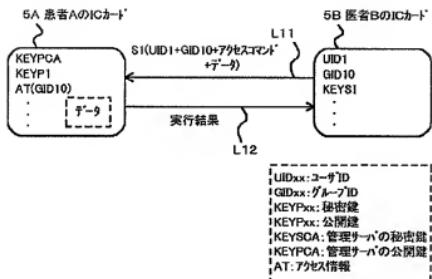
  

(B) グループIDとアクセス情報	
グループID	名前情報
	読み出可
	住所情報
	読み出可
GID10	カルテ情報
	読み出／書き込可
	施設情報
	読み出／書き込可
...	...
...	...
...	...
...	...

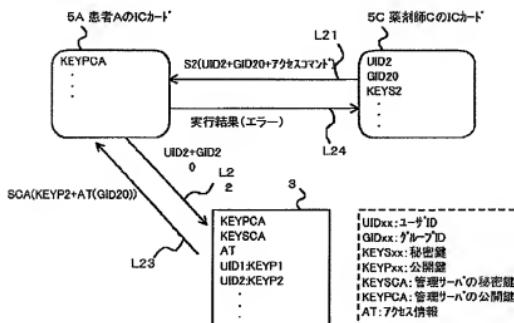
【図8】



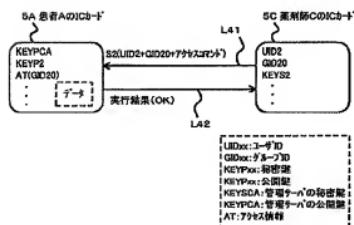
【図9】



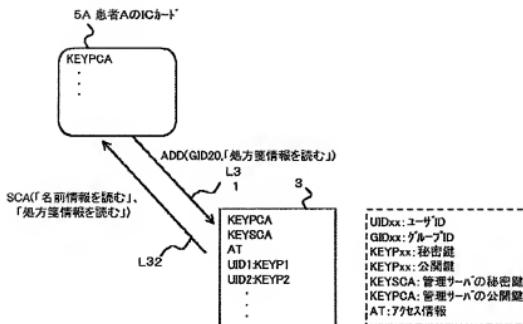
【図10】



【図12】



【図11】



## フロントページの続き

(51)Int.CI. <sup>7</sup>	調査記号	F I	フロント (参考)
G 0 9 C	6 6 0	G 0 6 K	19/00
H 0 4 L	9/32	H 0 4 L	9/00
		P	6 7 5 B

(72)発明者 町田 修  
東京都江東区農糸三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

F ターム (参考) 5B035 AA00 BB09 BC01 CA38  
5B058 CA27 KA02 KA04 KA33 YA20  
5B085 AE12 AE13 AE23 BC07  
5J104 AA07 AA09 AA12 EA26 KA02  
KA05 LA03 LA06 MA02 MA06  
NA02 NA20 NA35 NA36 NA40  
PA07  
9A001 BB05 EE03 JZ25 JZ27 KZ58  
KZ60 KZ61 LL03